ON THE NON-COMMUTATIVE ENDOMORPHISM RINGS OF ABELIAN SURFACES

JAMES STANKEWICZ

Abstract. A conjecture of Coleman implies that only finitely many quaternion algebras over the rational numbers can be the endomorphism $\mathbf{Q}$-algebras of abelian surfaces over the complex numbers which can be defined over $\mathbf{Q}$. One may think of this as a higher-dimensional version of the Gauss Class Number problem. Before now, no one has ruled out quaternion algebras over $\mathbf{Q}$ not already ruled out by the Albert classification. We rule out infinitely many such quaternion algebras by showing that for infinitely many D, the Atkin-Lehner quotient Shimura curve X^D/w_D has no $\mathbf{Q}$-rational points. Our principal method is to use the level structure maps above X^D to create torsors for use in the descent obstruction. Numerous Diophantine and analytic results on Shimura curves are also proved.

1. Introduction

Consider the Gauss class number problem. In his *Disquisitiones* [Gau86], Gauss computed the number of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of positive-definite binary quadratic forms over the integers with discriminant Δ for many $\Delta < 0$. He found a composition law for these classes and conjectured that for $\Delta < -163$ there is always more than one class. This composition law is essentially the multiplication of invertible ideal classes in $\mathbf{Z}[(\Delta + \sqrt{\Delta})/2]$. Therefore a solution to this problem would also show that there are precisely 9 imaginary quadratic fields of class number one. A solution was given independently in the mid-1900s by Heegner [Hee52], Baker [Bak68], and Stark [Sta67]. There is a third interpretation of this problem, namely that of elliptic curves with complex multiplication or CM [Sil86, §C.11]. In particular, they also showed that if an elliptic curve $E_{/\mathbf{Q}}$ has CM then it has CM by one of these 9 imaginary quadratic fields. We note here that it would be somewhat more precise to say that such a curve has *potential* CM because it is only over fields $F \supset K = \mathbf{Q}(\sqrt{\Delta})$ that we have $\mathbf{Q} \otimes \mathrm{End}(E_F) \cong K$ where E_F denotes the base change.

Let $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbf{Q}$ for A an abelian variety. The Albert classification [BL04, §5.5] tells us that if A is defined over $\mathbf{Q}$, $\dim(A) = 2$ and $\mathrm{End}^0(A)$ is not commutative, then $\mathrm{End}^0(A_{\overline{\mathbf{Q}}})$ must be either a quaternion algebra over $\mathbf{Q}$ which embeds into $M_2(\mathbf{R})$ or the two-by-two matrices over an imaginary quadratic field. In fact, there should be only finitely many possibilities. It was conjectured by Coleman that for any fixed dimension g, there are only finitely many $\mathbf{Z}$-algebras which can be $\mathrm{End}(A_{\overline{\mathbf{Q}}})$ for any g-dimensional abelian variety over $\mathbf{Q}$ [BFGR06, Conjecture C(1,g)]. This is an extremely hard conjecture which will probably not see a resolution in the near future. There are very few techniques for ruling out a given endomorphism algebra which is not specifically ruled out by Albert's classification. Until now, none have succeeded in ruling out any such quaternion algebras over

$\mathbf{Q}$. For the following, recall that the discriminant D of a quaternion algebra $B_{/\mathbf{Q}}$ identifies a quaternion algebra up to isomorphism and D is positive if and only if the associated quaternion algebra embeds into $M_2(\mathbf{R})$ [Cla03, p.20].

Theorem 1.1. *There is a constant $c > 0$ such that among the integers $0 < D < X$, there are $\geq cX/\log(X)$ which are discriminants of a quaternion algebra $B_{/\mathbf{Q}}$ where for all principally polarized abelian surfaces $A_{/\mathbf{Q}}$, $B \not\hookrightarrow \mathrm{End}^0(A_{\overline{\mathbf{Q}}})$.*

That is to say, we rule out a nearly positive proportion of all possible quaternion algebras over $\mathbf{Q}$. To solve this problem, we turn it into a question about rational points and moduli spaces. We mention some past work in this direction. Shimura showed [Shi75] that if we change $\mathrm{End}^0(A_{\overline{\mathbf{Q}}})$ to $\mathrm{End}^0(A)$, then there are no non-commutative endomorphism rings at all, similarly to how the CM of an elliptic curve over $\mathbf{Q}$ can only be *potential*. In particular, if D is the discriminant of a quaternion algebra $B \subset M_2(\mathbf{R})$, we let X^D be the coarse moduli space of principally polarized abelian surfaces A with an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ where $\mathcal{O}$ is a *maximal order* in B. From ι, we can define a principal polarization on A in a canonical but not unique way. We mean this to be a scheme X^D defined over the integers, and so use $X^D_{\mathbf{Q}}$ to refer to its base change. Shimura showed that if B is division, then $X^D(\mathbf{R}) = \emptyset$, and we may think of this as saying the action of $\mathcal{O}$ cannot be defined over $\mathbf{R}$. If we take the quotient of X^D by *Atkin-Lehner involutions* w_m [Sta14, Definition 2.2], we remove this ambiguity. Work of Rotger [Rot04, Theorem 3.5] shows how we can use this non-uniqueness to find an explicit quotient M^D of $(X^D/w_D)_{\mathbf{Q}}$ such that if $M^D(\mathbf{Q}) = \emptyset$ then $B \not\hookrightarrow \mathrm{End}^0(A_{\overline{\mathbf{Q}}})$ for *all* principally polarized abelian surfaces over $\mathbf{Q}$ [Cla03, Corollary 84]. In the cases where we prove the lack of rational points (when the quaternion algebra B of discriminant D is *non-twisting* in the sense of Rotger [Rot04, Definition 3.2]), we will in fact have $M^D = (X^D/w_D)_{\mathbf{Q}}$. What makes this difficult, and has prevented progress in the past, is a Theorem of Clark [Cla03, Main Theorem 2] that $M^D(\mathbf{Q}_v) \neq \emptyset$ for all places v of $\mathbf{Q}$. Consequently, if $M^D(\mathbf{Q}) = \emptyset$ then M^D is a *counterexample to the Hasse principle*. We do not, except in small cases, know equations for M^D or X^D so we cannot hope to attack the problem in that manner. This is part of the reason that there has been very little progress on this problem since the theorems of Clark and Rotger. Instead, we use a three part process to step down to $(X^D/w_D)(\mathbf{Q})$ and show it is empty for infinitely many D: an important Diophantine problem in its own right.

Recall that if $V_{/\mathbf{Q}}$ is a variety, a twist of V is a variety $V'_{/\mathbf{Q}}$ such that $V_{\overline{\mathbf{Q}}} \cong V'_{\overline{\mathbf{Q}}}$. We say that V' is a quadratic twist if there is a quadratic field $K/\mathbf{Q}$ such that $V_K \cong V'_K$. If we can show that all quadratic twists of $X^D_{\mathbf{Q}}$ have no rational points, we can show that $(X^D/w_D)(\mathbf{Q})$ is empty and Theorem 1.1 will have been proved. This step down from quadratic twists of $X^D_{\mathbf{Q}}$ to $(X^D/w_D)_{\mathbf{Q}}$ is Lemma 4.5.

To deal with quadratic twists of $X^D_{\mathbf{Q}}$, we use the *descent obstruction* [Sko01, Definition 5.3.1]. Namely, associated to a torsor f above our quadratic twist, we find a set $\kappa(f)$ containing the rational points of our quadratic twist. The furthest this idea has been explored in previous literature has been to use the Shimura covering for the torsor f [Sko05, dVP13] to produce a single twist of X^{2641} which violates the Hasse principle [RSY05]. We note that this example does not show anything about abelian surfaces and the quaternion algebra of discriminant 2641 as the twist is by the wrong involution. To get all quadratic twists by the appropriate

involution w_D we need a truly new idea. We find it in considering the Shimura variety structure associated to the X^D moduli problem - namely a limit of covers of $X^D_{\mathbf{Q}}$ given by level structures. Under some conditions on D, these covers are étale, and provide a torsor f. In section 3 we show how to port these *level structure torsors* over to twists of $X^D_{\mathbf{Q}}$. If we can show the obstruction set κ associated to the level structure torsors is empty, we will have shown both Theorem 1.1 and the following.

Theorem 1.2. *There are infinitely many D for which there is a twist T of X^D which violates the Hasse principle and is explained by the descent obstruction. In particular, there are real numbers $c_D, e_D > 0$ and a subset of the integers $-X < d < 0$ of size $c_D X/\log^{e_D}(X) + O(X/\log^{e_D+1}(X))$ such that there is a twist T satisfying $T_{\mathbf{Q}(\sqrt{d})} \cong X^D_{\mathbf{Q}(\sqrt{d})}$.*

The set of d in Theorem 1.2 can be explicitly described in terms of congruence conditions and is nearly optimal, as we will see when we prove Theorem 1.2 in §5. The congruence conditions are what allow us to get such precise asymptotics, as we may thus use Dirichlet L-functions in the style of Serre and Watson [Ser76, Wat35]. The resulting twists of X^D are explicitly defined in terms of d and Atkin-Lehner involutions [Sta14, Definition 2.2]. It is tempting to think, after work of Bhargava, that the Hasse principle should almost always fail [Bha]. It is worth keeping in mind however that Bhargava's work applies only to hyperelliptic curves, which are very special. Among other things, a hyperelliptic curve H given by the equation $y^2 = f(x)$ always has a quadratic twist with a rational point. For instance, if H has no rational points then $f(1) \neq 0$ but the curve given by $f(1)y^2 = f(x)$ obviously has rational points. The case of Shimura curves is rather different. The top step in our method will be showing that a family of Shimura curves above X^D do not even have p-adic points on any twists. This is somewhat technical and builds on previous results of the author [Sta14], but it can be used to show that the descent set κ is empty and thus prove Theorems 1.1 and 1.2.

The outline of the paper therefore follows: we start at the top, finding families of Shimura curves for which *all* twists lack p-adic points for some p. We then show how to find level structure torsors above twists of $X^D_{\mathbf{Q}}$. We then show how this applies to the descent obstruction, and step down to rational points on twists of $X^D_{\mathbf{Q}}$. We will then step down to rational points on $(X^D/w_D)_{\mathbf{Q}}$. We give applications to abelian varieties and prove Theorem 1.1 in §4. Finally, we give the asymptotics for Theorem 1.2.

It is the authors pleasure to acknowledge the helpful conversations about this work with Jon Bober, Pete L. Clark, Lars Halle, Ian Kiming, Alexei Skorobogatov, and John Voight. The author was partially supported by the Villum Fonden through the network for Experimental Mathematics in Number Theory, Operator Algebras and Topology at the University of Copenhagen.

2. A technical theorem on p-adic points

Our method for proving Theorem 1.1 will be to show that every twist of X^D lacks $\mathbf{Q}$-points. To do this, we will study the p-adic points on a Shimura curve which is also an étale cover of X^D. Let N be an integer coprime to D, and consider the Shimura curve $X^D_0(N)$ [Sta14, Definition 2.1]. There is a natural map $X^D_0(p) \to X^D$ for all primes p, and Lemma 2.2 tells us when this map is étale after base change to

$\mathbf{Q}$. Both $X_{\mathbf{Q}}^D$ and $X_0^D(p)_{\mathbf{Q}}$ come naturally endowed with a commutative, $\mathbf{Q}$-rational group of involutions called the Atkin-Lehner involutions [Sta14, Definition 2.2]. Let $\omega(n)$ be the number of distinct prime divisors of n and $\mathrm{Gal}_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The group of Atkin-Lehner involutions of $X_{\mathbf{Q}}^D$ and $X_0^D(p)_{\mathbf{Q}}$ are respectively $(\mathbf{Z}/2)^{\omega(D)}$ and $(\mathbf{Z}/2)^{\omega(Dp)}$. The group of automorphisms of a variety $V_{/\mathbf{Q}}$ naturally determines its twists, in that the pointed set of isomorphism classes of twists of V is isomorphic to the pointed set $H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathrm{Aut}(V_{\overline{\mathbf{Q}}}))$ [Sil86, Theorem X.2.2].

If X is a positive integer and $p \equiv 1 \bmod 4$ is a prime, we will give in Definition 2.14 a set $S_p(X)$ of integers $0 < D < X$ with $p \nmid D$ such that $\#S_p(X) \gg X/\log(X)$ and such that for all twists T of $X_0^D(p)$, $T(\mathbf{Q}_p) = \emptyset$. The union over all $p \equiv 1 \bmod 4$ of the S_p is the set implicitly defined by Theorem 1.1. We will see in §4 that the following theorem will allow us to show for all twists U of $X_{\mathbf{Q}}^D$ that $U(\mathbf{Q})$ is empty.

Theorem 2.1. *For all primes $p \equiv 1 \bmod 4$ and all positive integers X, there is a set $S_p(X)$ of square-free positive integers $D \leq X$ such that $\#S_p(X) \gg X/\log(X)$ and for all twists T of $X_0^D(p)_{\mathbf{Q}}$, if $D \in S_p(X)$ then $T(\mathbf{Q}_p) = \emptyset$.*

In order to prove Theorem 2.1, we will use Lemma 2.3 to determine when $\mathrm{Aut}(X_0^D(p)_{\mathbf{Q}})$ is made up entirely of Atkin-Lehner involutions. We first concentrate on the twists of $X_0^D(p)_{\mathbf{Q}}$ by a quadratic field $K/\mathbf{Q}$, i.e. the twists T such that $T_K \cong X_0^D(p)_K$. If p is split in K, we give conditions to show that $T(\mathbf{Q}_p) = \emptyset$ in §2.1. If p is inert in K, we will give conditions to show that $T(\mathbf{Q}_p) = \emptyset$ in §2.2. If p is ramified in K we will give conditions to show that $T(\mathbf{Q}_p) = \emptyset$ in §2.3. We will show in §2.4 that if we impose all these conditions on D and p then for all twists T of $X_0^D(p)_{\mathbf{Q}}$, $T(\mathbf{Q}_p) = \emptyset$. Let us recall some facts about X^D and $X_0^D(p)$ which allow us to put all quadratic twists into a normal form.

Lemma 2.2. *The following are equivalent.*

1. *There are primes $q, q' \mid D$ (possibly equal) such that $q \equiv 1 \bmod 4$ and $q' \equiv 1 \bmod 3$.*
2. *For all primes $\ell \nmid D$, the natural map $X_0^D(\ell)_{\mathbf{Q}} \to X_{\mathbf{Q}}^D$ is étale.*
3. *For all primes $\ell \nmid D$, there are exactly two components of $X_0^D(\ell)_{\overline{\mathbf{F}}_\ell}$.*

Proof. The natural map $X_0^D(\ell) \to X^D$ is étale over $\mathbf{Q}$ if and only if the base change to $\mathbf{C}$ is a covering space map of Riemann surfaces [Sta15, Tag 02GJ]. For any D and ℓ, the branch locus lies inside the locus of cusps and elliptic points. If $D > 1$ there are no cusps and there can only be elliptic points of order 2 or 3. Respectively, the number of these is a product over the prime divisors of D easily obtained from the genus formula [Cla03, Proposition 46] as

$$\prod_{q \mid D} \left(1 - \left(\frac{-4}{q}\right)\right), \prod_{q \mid D} \left(1 - \left(\frac{-3}{q}\right)\right).$$

Meanwhile, the exceptional components of $X_0^D(\ell)_{\overline{\mathbf{F}}_\ell}$ come in chains of one or two copies of $\mathbb{P}^1_{\overline{\mathbf{F}}_\ell}$. It can be determined from a calculation with supersingular points [Mol12, Theorem 1.1] that the number of chains of one or two components is respectively a nonzero constant times

$$\prod_{q \mid D\ell} \left(1 - \left(\frac{-4}{q}\right)\right), \prod_{q \mid D\ell} \left(1 - \left(\frac{-3}{q}\right)\right).$$

□

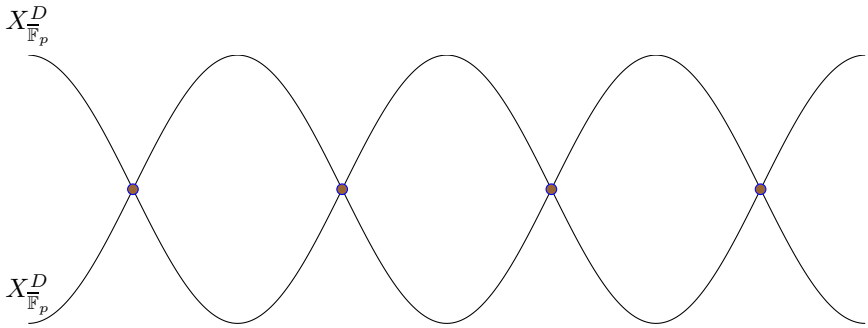

FIGURE 1. $X_0^D(p)_{\overline{\mathbb{F}}_p}$

We note that if D satisfies the conditions of Lemma 2.2 then the components of $X_0^D(p)_{\overline{\mathbb{F}}_p}$ will be joined precisely at the supersingular points as in Figure 1 [Sta14, Theorem 2.8].

Lemma 2.3. *For D as in Lemma 2.2, the only automorphisms of $X_0^D(N)_{\mathbf{Q}}$ for any N such that DN is square-free are the Atkin-Lehner involutions.*

Proof. This follows from work of Rotger [Rot02, Theorem 2]. □

If D satisfies the conditions of Lemma 2.2 then we let $W = \mathrm{Aut}(X_0^D(p)_{\overline{\mathbf{Q}}}) \cong (\mathbf{Z}/2\mathbf{Z})^{\omega(Dp)}$, the group of Atkin-Lehner involutions. For a divisor m of Dp we will let w_m denote the corresponding automorphism of $X_0^D(p)$ [Sta14, Definition 2.2]. The group W is commutative and each element is $\mathbf{Q}$-rational so $H^1(\mathrm{Gal}_{\mathbf{Q}}, W) = \mathrm{Hom}(\mathrm{Gal}_{\mathbf{Q}}, W)$. If $K = \mathbf{Q}(\sqrt{d})$ is a quadratic field extension of $\mathbf{Q}$ then we have an isomorphism $\mathrm{Gal}(K/\mathbf{Q}) \to \langle w_m \rangle$ for any Atkin-Lehner involution w_m. This isomorphism induces a cocycle $\xi_{m,d} : \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{Aut}(X_0^D(p)_{\mathbf{Q}})$ which therefore defines a twist [BLR90, Example 6.1.B].

Definition 2.4. Let $C^D(p, d, m)$ be the twist of $X_0^D(p)_{\mathbf{Q}}$ defined by $\xi_{m,d}$.

2.1. **The Split Case.** Throughout this section, we will take p to be an odd prime. We will also let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field in which p splits. We will always let D be the (reduced) discriminant of an indefinite quaternion algebra, namely the square-free product of an even number of primes. For simplicity we will also assume D is odd.

Definition 2.5. We say that D is *non-ordinary* at $p \nmid D$ if for all s in $\{1, \ldots, \lfloor\sqrt{4p}\rfloor\}$ there exists a prime $q_s \mid D$ such that $\left(\dfrac{s^2 - 4p}{q_s}\right) = 1$.

This terminology comes from the fact that if D is non-ordinary at p, then there are no $\mathbb{F}_p$-rational ordinary points on X^D. This is to say, considering Figure 1, that the smooth locus of $X_0^D(p)(\mathbb{F}_p)$ is empty. This is not a particularly hard condition for D to satisfy, and it is defined in terms of congruence conditions. For example, if $p = 5$ then $s^2 - 4p \in \{-19, -16, -11, -4\}$ and $\left(\dfrac{s^2 - 20}{137}\right) = 1$ for all s. Therefore if q is any prime, $D = 137q$ is non-ordinary at 5.

Theorem 2.6. *If p is a prime and D satisfying the conditions of Lemma 2.2 is non-ordinary at p then $X_0^D(p)(\mathbf{Q}_p) = \emptyset$. Moreover, if p splits in K then for all twists T of $X_0^D(p)_{\mathbf{Q}}$ by K we have $T(\mathbf{Q}_p) \neq \emptyset$.*

The proof of this relies on the Eichler-Selberg trace formula [Eic56]. We make this precise using the following definition.

Definition 2.7. Let p be a prime and let $\Delta < 0$ such that $\Delta \mod 4 \in \{0, 1\}$. If we let $\left(\frac{\Delta}{p}\right)$ be the Kronecker symbol and $f(\Delta)$ the conductor of $\mathbf{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$ then we define the Eichler symbol as

$$\left\{\frac{\Delta}{p}\right\} = \begin{cases} 1 & p \mid f(\Delta) \\ \left(\frac{\Delta}{p}\right) & else. \end{cases}$$

We note that we can also consider even D by replacing the Kronecker symbol in Definition 2.5 by the Eichler symbol.

Proof. If p splits in K, we have an embedding $K \hookrightarrow \mathbf{Q}_p$. Since $T_K \cong X_0^D(p)_K$, we have $T_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. We can see that $X_0^D(p)$ has no p-adic points if and only if a certain quantity $TF'(D, p, 1, p)$ vanishes [Sta14, Theorem 6.1(a)]. This quantity vanishes if D is non-ordinary at p because $TF'(D, p, 1, p)$ can be explicitly realized as

$$2 \sum_{s=1}^{\lfloor\sqrt{4p}\rfloor} \sum_{f \mid f(s^2-4p)} H(s, f) \prod_{q \mid D} \left(1 - \left\{\frac{(s^2-4p)/f^2}{q}\right\}\right),$$

where $H(s, f)$ is an explicit nonzero constant [RSY05, Corollary 2.4]. It suffices to require that $\left(\frac{s^2-4p}{q_s}\right) = 1$ because if so, $q_s \nmid s^2 - 4p$ and so $q_s \nmid f$, $\left(\frac{f^2}{q_s}\right) = 1$, and

$$\left(\frac{(s^2-4p)/f^2}{q_s}\right) = \left\{\frac{(s^2-4p)/f^2}{q_s}\right\} = 1.$$

□

2.2. **The Inert Case.** Now let p be inert in $K = \mathbf{Q}(\sqrt{d})$ and let D be odd and coprime to p, satisfying the conditions of Lemma 2.2. Here we vitally use Lemma 2.3 to say that each twist by K is of the form $C^D(p, d, m)$ (as in Definition 2.4) for some $m \mid Dp$, and in this section we always assume $m \neq 1$ so that $C^D(p, d, m) \ncong X_0^D(p)_{\mathbf{Q}}$. For $m \mid D$ we can mimic §2.1 and study the ordinary points in $X_0^D(p)(\overline{\mathbb{F}}_p)$ which become $\mathbb{F}_p$-rational on $C^D(p, d, m)$. The number of these is a quantity $TF'(D, p, m, p)$ coming from the Eichler-Selberg trace formula [Sta14, Lemma 6.14]. For $\Delta = \Delta(s, f, m) = (s^2 - 4pm)/f^2 \in \mathbf{Z}_{<0}$ such that $4 \mid \Delta(\Delta - 1)$, there is an explicit nonzero constant $H(s, f, m)$ [RSY05, Corollary 2.4], [Sta14, Definition 6.13] such that

$$TF'(D, p, m, p) = 2 \sum_{s=1}^{\lfloor\sqrt{4pm}\rfloor} \sum_{f} H(s, f, m) \prod_{q \mid D} \left(1 - \left\{\frac{\Delta}{q}\right\}\right).$$

If we want to guarantee this quantity is zero for all m, we need to at least make sure that if $m = D$ and $q \mid D$, then $q \nmid s$ when $s^2 < 4Dp$. If $q \mid s$ for some $q \mid D$ then

$\prod_{q|D}\left(1-\left\{\frac{s^2-4Dp}{q}\right\}\right)=1$, which we need to avoid. In fact the problem persists for all $m \mid D$. We fix the problem by restricting to the following D.

Definition 2.8. If $q \mid D$ is a prime then we define $P_D(q)$ to be the product of all primes $q' \mid D$ such that $q' < q$. We say that D is *spaced out* at p if for all primes $q \mid D$, we have $q > 4pP_D(q)$.

Lemma 2.9. *Suppose D is spaced out at p. If $m \mid D$, then $TF'(D,p,m,p)=0$.*

Proof. Let $q \mid m \mid D$ be an odd prime such that $q \mid s^2-4pm$ for some $0<s^2<4pm$. Set $\nu=(s^2-4pm)/q<0$ and $\tau=s/q$. Thus $q^2\tau^2=q(\nu+4pm/q)$ and so $q \le q\tau^2=\nu+4pm/q<4pm/q$.

Suppose now D is spaced out at p and let q be the largest prime dividing m. It follows that $q>4pP_D(q)\ge 4pm/q$ and so $q \nmid s^2-4pm$ for all s such that $0<s^2<4pm$. For any fixed s, let $t_s=q-s$ and $n_s=2s-q-4pm/q$. It follows that

$$\begin{aligned} s^2-4pm &= s^2+q(-4pm/q+q-q+2s-2s) \\ &= s^2-2sq+q^2+q(-4pm/q-q+2s) \\ &= (q-s)^2+q(2s-q-4pm/q) \\ &= t_s^2+qn_s. \end{aligned}$$

We see that $\left(\frac{s^2-4pm}{q}\right)=1$ for all s because q is odd and there is an integer t such that $q \nmid t$ and $s^2-4pm \equiv t^2 \bmod q$. To complete the proof, note that since $q \nmid s^2-4pm$, $q \nmid f$ and therefore there exists an integer f' such that $ff' \equiv 1 \bmod q$ and so $(s^2-4pm)/f^2 \equiv (t_sf')^2 \bmod q$. □

Theorem 2.10. *If D is spaced out at p and p is inert in K then all twists T of $X_0^D(p)_{\mathbf{Q}}$ by K have no $\mathbf{Q}_p$-points.*

Proof. By Lemma 2.3 any such twist must be of the form $C^D(p,d,m)$ for some $m \mid Dp$. If $p \mid m$ there are no smooth $\mathbb{F}_p$-rational points because the two branches of $X_0^D(p)_{\overline{\mathbb{F}}_p}$ are interchanged by the new action of Frobenius. If $p \nmid m$ then by Lemma 2.9, $TF'(D,p,m,p)=0$ and there are no smooth $\mathbb{F}_p$-rational points. In either case, Hensel's Lemma [JL85, Lemma 1.1] completes the proof. □

Remark 2.11. We note a general framework here. Previous results [Sta14, Corollary 3.17] show that we can always make a twist of X^D such that a supersingular point becomes $\mathbb{F}_p$-rational if $p \nmid D$. Therefore our only chance to prevent $\mathbf{Q}_p$ points is to make these points non-smooth on the special fiber [JL85, Lemma 1.1]. This is to say that we need to move from X^D to $X_0^D(p)$, so that the supersingular points become singular as in Figure 1. Moving back from $X_0^D(p)$ to X^D, where our points become smooth again is essentially what lets us produce *Counterexamples to the Hasse principle* instead of just curves without rational points.

2.3. **The Ramified Case.** Suppose now that p is ramified in $\mathbf{Q}(\sqrt{d})$, i.e. that $p \mid d$ since p is odd. In fact, if $D=q_1 \dots q_{2n}$ we will let $p \equiv q_1 \equiv \dots \equiv q_{2n} \equiv 1 \bmod 4$ for convenience. As before we let $C^D(p,d,m)$ be as in Definition 2.4. If p is ramified, a regular model for $C^D(p,d,m)$ looks far different from the regular model

for $X_0^D(p)_{\mathbf{Q}}$, whose special fiber is depicted in Figure 1. The construction of a regular model will be of primary concern in this section. Once we have that, our conditions for preventing rational points will follow from a formula for the number of Atkin-Lehner fixed points on $X^D_{\overline{\mathbb{F}}_p}$ and Hensel's lemma. Indeed, the number of fixed points will be a nonzero multiple of the number of reduced components on the regular model over $\overline{\mathbb{F}}_p$. We will divide our work into the case when $p \mid m$ and when $p \nmid m$. The latter case will be further divided into the case when $\left(\frac{-m}{p}\right) = 1$ or not.

In all cases, we form a regular model $\mathcal{X}_{/\mathbf{Z}_p}$ by taking a quotient of the regular model $\mathcal{Y}$ of $X_0^D(p)$ over $\mathbf{Z}_p[\sqrt{d}]$ to obtain a normal model $\mathcal{Z}_{/\mathbf{Z}_p}$ and resolving its singularities [Lor14]. In particular, if $\langle\sigma\rangle = \mathrm{Gal}(\mathbf{Q}_p(\sqrt{d})/\mathbf{Q}_p)$ then we take the quotient by $H = \langle h = \sigma w_m\rangle$. Since each w_m acts on $X_0^D(p)$, there is a corresponding automorphism on $\mathcal{Y}, \mathcal{Z}$, and $\mathcal{X}$ which we will also refer to as w_m by abuse of notation. We also let $H_\Delta(X)$ denote the Hilbert Class polynomial for $\mathbf{Z}[(\Delta+\sqrt{\Delta})/2]$ and $h(\Delta) = \deg(H_\Delta)$.

2.3.1. *A regular model when $p \nmid m$.* If $m \mid D$ and $p \mid d$, $C^D(p, d, m)$ has a normal model $\mathcal{Z}$ with a non-reduced special fiber [Sta14, §4.1]. More precisely, as a divisor on $\mathcal{Z}$, $\mathcal{Z}_{\overline{\mathbb{F}}_p} = 2(\Gamma + \Gamma')$ where $\Gamma \cong \Gamma' \cong (X^D/w_m)_{\overline{\mathbb{F}}_p}$, intersecting at the images of the supersingular points of X^D. See Figure 2 for a depiction. The set of ramification points of $\mathcal{Y} \to \mathcal{Z}$ is the collection of fixed points of w_m on $\mathcal{Y}_{\mathbb{F}_p}$, which we identify with the w_m-fixed points on $\mathcal{Z}_{\mathbb{F}_p}$. Since $-m \equiv 3 \bmod 4$, there are $h(-4m)\prod_{q|D}\left(1 - \left\{\frac{-4m}{q}\right\}\right)$ fixed points of w_m on $X^D(\mathbf{C})$ and thus on each branch of $\mathcal{Y}(\overline{\mathbb{F}}_p)$ by the Grothendieck-Lefschetz fixed point formula on X^D. Note that we do not have the same formula if $p = 2$. Since p is odd, the total number of w_m-fixed points in $\mathcal{Y}(\overline{\mathbb{F}}_p)$ and thus $\mathcal{Z}(\overline{\mathbb{F}}_p)$ depends on whether the w_m-fixed points are in the smooth locus of $\mathcal{Y}$.

If $\left(\frac{-m}{p}\right) = 1$ then the fixed points of w_m on $\mathcal{Y}(\overline{\mathbb{F}}_p) \cong X_0^D(p)(\overline{\mathbb{F}}_p)$ occur in the ordinary (and thus smooth) locus of $\mathcal{Y}$. In particular, we may localize away from one of the components of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ before blowing up. We see that this is the essentially the same regular model as in the case of good reduction [Sta14, Theorem 4.1.1-2]. This is to say that we have smooth $\mathbb{F}_p$-rational points if and only if we have $\mathbb{F}_p$-rational w_m-fixed points in $X^D(\overline{\mathbb{F}}_p)$. Over $\overline{\mathbb{F}}_p$ these correspond in a 2:1 fashion to the reduced components of $\mathcal{X}_{\overline{\mathbb{F}}_p}$. A depiction of the regular model $\mathcal{X}$ is given in Figure 3 where s denotes the strict transform under the blowup.

If $\left(\frac{-m}{p}\right) = -1$ then the fixed points of w_m on $\mathcal{Y}(\overline{\mathbb{F}}_p)$ are supersingular and hence lie on the intersection points of the two branches of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$. Hence the completion of the strict henselization of the local ring at any fixed point of w_m on $\mathcal{Y}_{\mathbb{F}_p}$ is

$$A \cong \mathbf{Z}_p^{nr}[\![t_1, t_2, t_3]\!]/(t_1t_2 - p, t_3^2 - p).$$

Further, since the action of w_m on each branch is nontrivial, we may linearize the action of h so that $h(t_i) = -t_i$. A basis for the invariants of this action is therefore the degree 2 monomials in the t_i and the ones which don't already lie in $\mathbf{Z}_p^{nr}$ are $x_1 = t_1^2$, $x_2 = t_2^2$, $x_3 = t_1t_3$, and $x_4 = t_2t_3$. Therefore the strict henselization of the

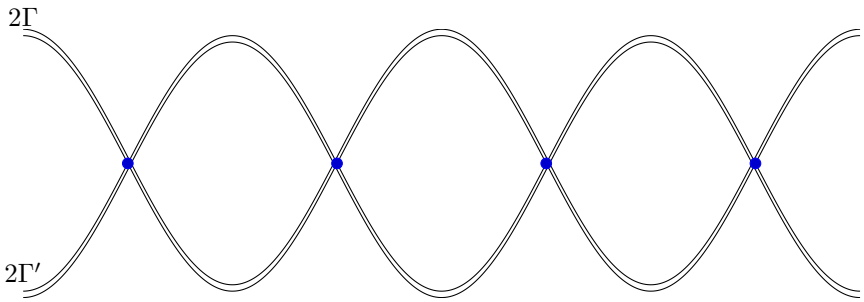

FIGURE 2. $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ when $p \nmid m$

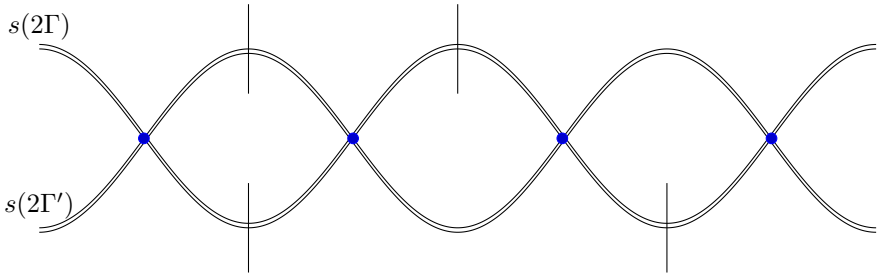

FIGURE 3. A regular model in the ordinary case when $p \nmid m$.

local ring of $\mathcal{Z}$ at the image of a w_m-fixed point is

$$A^H \cong \frac{\mathbf{Z}_p^{nr}[\![x_1, x_2, x_3, x_4]\!]}{(px_1 - x_3^2, px_2 - x_4^2, px_3 - x_1x_4, px_4 - x_2x_3, p^2 - x_1x_2, p^2 - x_3x_4)}.$$

This is not a regular ring, but the blowup of $\mathrm{Spec}(A^H)$ is and there is a reduced component in $\mathcal{X}_{\overline{\mathbb{F}}_p}$ above the image in $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ of a w_m-fixed point. A depiction of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is given in Figure 4 where s denotes the strict transform under the blowup. Therefore $\mathcal{X}(\mathbb{F}_p)$ is nonempty if and only if there is an $\mathbb{F}_p$-rational w_m-fixed point on $\mathcal{Y}_{\mathbb{F}_p}$. In fact, since these fixed points occur in the nonsmooth locus, it suffices to count the number of these on a single branch of $\mathcal{Y}_{\overline{\mathbb{F}}_p}$. We have thus reduced ourselves to a case where numerical conditions have already been established [Sta14, Theorem 4.1.3-6].

2.3.2. *A regular model when $p \mid m$.* If on the other hand $p \mid m$ then for the normal model $\mathcal{Z}$, $\mathcal{Z}_{\overline{\mathbb{F}}_p} = 2\Gamma''$ with $\Gamma'' \cong X^D_{\overline{\mathbb{F}}_p}$. Recall that when $p \mid m$ all fixed points are supersingular. So once more the strict henselization of the local ring at any fixed point of w_m on $\mathcal{Y}_{\mathbb{F}_p}$ is $A \cong \mathbf{Z}_p^{nr}[\![t_1, t_2, t_3]\!]/(t_1t_2 - p, t_3^2 - p)$. We can linearize the action to have $h(t_3) = -t_3$, $h(t_1) = t_2$ and $h(t_2) = t_1$. A basis for the invariants of this action is thus $x = t_1 + t_2$ and $y = t_3(t_1 - t_2)$. Therefore $A^H \cong \mathbf{Z}_p^{nr}[\![x, y]\!]/(y^2 - p(x^2 - 4p))$ is the completion of the strict henselization of the local ring of the image of a w_m-fixed point on $\mathcal{Z}$. A succession of blowups resolves this singularity and a partial depiction of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is given in Figure 2.3.2. Therefore $\mathcal{X}(\mathbb{F}_p)$ is nonempty if and only if there is an $\mathbb{F}_p$-rational w_m-fixed point in $\mathcal{Y}(\overline{\mathbb{F}}_p)$. Since $p \mid m$ is odd

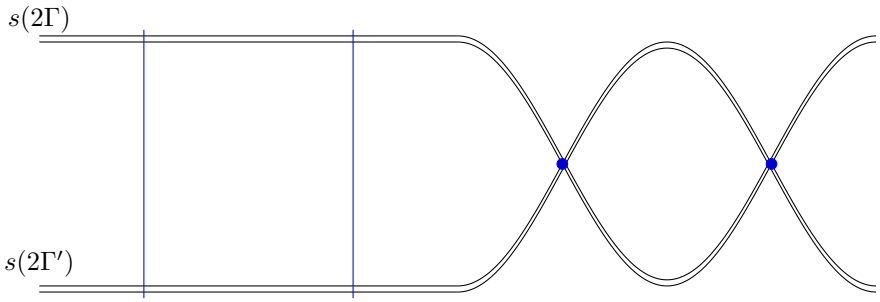

FIGURE 4. A regular model in the supersingular case when $p \nmid m$.

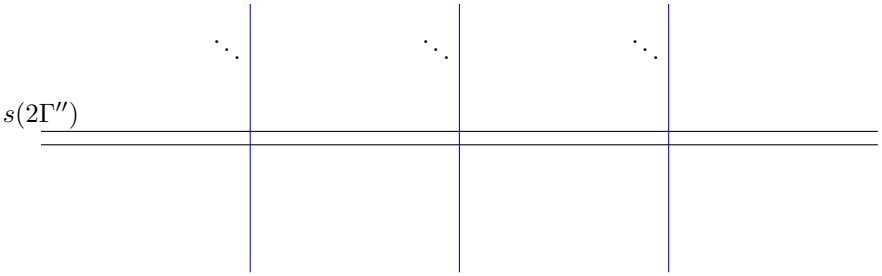

FIGURE 5. A regular model when $p \mid m$.

and $-m \equiv 3 \bmod 4$, there are $h(-4m/p)\prod_{q|D}\left(1-\left\{\frac{-4m/p}{q}\right\}\right)$ fixed points of w_m in $\mathcal{Y}(\overline{\mathbb{F}}_p)$. But then we already know whether any of these are $\mathbb{F}_p$-rational [Sta14, Theorem 4.1.3-6].

2.3.3. *Rationality results.* We now use our newly-formed regular models to rule out rational points on ramified twists. In particular, by Hensel's Lemma [JL85, Lemma 1.1], if the smooth locus of $\mathcal{X}(\mathbb{F}_p)$ is empty, then $\mathcal{X}(\mathbf{Q}_p) = C^D(p,d,m)(\mathbf{Q}_p)$ is empty. In fact, we show that unless $m = D$ or Dp then the smooth locus of $\mathcal{X}(\overline{\mathbb{F}}_p)$ is empty by restricting to the D satisfying the following condition.

Definition 2.12. Let $D = q_1 \dots q_{2n}$ for $n \geq 1$ with $q_1 \equiv \dots \equiv q_{2n} \equiv 1 \bmod 12$. We say that D is *untangled* if for all $i \neq j$, $\left(\dfrac{q_i}{q_j}\right) = 1$.

The terminology here is inspired by the dictionary between primes and knots [Mor12]. Although we previously only required that $q_i \equiv 1 \bmod 4$, the condition $\left(\dfrac{q_i}{q_j}\right) = 1$ is relatively strong. We may as well require in our definition that the conditions of Lemma 2.2 are automatically satisfied.

Theorem 2.13. *If $p \equiv 1 \bmod 4$, D is untangled, $\left(\dfrac{D}{p}\right) = -1$, and $p \mid d$, then any nontrivial twist of $X_0^D(p)_{\mathbf{Q}}$ by $\mathbf{Q}(\sqrt{d})$ has no $\mathbf{Q}_p$ points.*

Proof. Since D is untangled, it satisfies the conditions of Lemma 2.3, so for any twist T of $X_0^D(p)_{\mathbf{Q}}$ there is an m such that $T \cong C^D(p,d,m)$. By the discussion in

§2.3.1, if $p \nmid m$ then the smooth locus of $\mathcal{X}(\mathbb{F}_p)$ is empty unless there are $\mathbb{F}_p$-rational w_m-fixed points on X^D [Sta14, Theorem 4.1]. This is to say, a numerical condition on the triple (D, m, p) is satisfied. In particular, if D is untangled, then none of the conditions are satisfied unless $m = D$. By the discussion in §2.3.2, if $p \mid m$ then $\mathcal{X}(\mathbb{F}_p)$ is empty unless the triple $(D, m/p, p)$ satisfies the same numerical condition. Again, if D is untangled then none of the conditions are satisfied unless $m = Dp$.

Suppose now $m = D$ or Dp so $\mathcal{X}(\mathbb{F}_p)$ contains no smooth points unless the triple (D, D, p) satisfies one of the following:

(1) $H_{-4D}(X) \bmod p$ has a root if $\left(\frac{D}{p}\right) = 1$ [Sta14, Theorem 4.1.1] or
(2) for all $q \mid D$, $\left(\frac{-p}{q}\right) = -1$ if $\left(\frac{D}{p}\right) = -1$ [Sta14, Theorem 4.1.3].

Since $\left(\frac{D}{p}\right) = -1$ we are in case 2, but for the same reason, there is some $q \mid D$ such that $\left(\frac{-p}{q}\right) = \left(\frac{p}{q}\right) = 1$. Therefore the triple (D, D, p) fails the numerical condition and $\mathcal{X}(\mathbb{F}_p)$ has no smooth points. Therefore $\mathcal{X}(\mathbf{Q}_p) = C^D(p, d, m)(\mathbf{Q}_p)$ is empty by Hensel's Lemma [JL85, Lemma 1.1]. □

2.4. **From Quadratic Twists to all twists.**

Definition 2.14. Let $p \equiv 1 \bmod 4$ be a prime. We let $S_p \subset \mathbf{Z}_{>0}$ be the set of integers D such that $\left(\frac{D}{p}\right) = -1$, D is untangled (Definition 2.12), D is spaced out at p (Definition 2.8), and D is non-ordinary at p (Definition 2.5). Similarly, we let $S_p(X) = S_p \cap \{1, 2, \ldots, X\}$ for any positive integer X.

If $D \in S_p$ then any *quadratic twist* of $X_0^D(p)_{\mathbf{Q}}$ has no $\mathbf{Q}_p$-points by Theorems 2.6, 2.10, and 2.13. In fact, we can now show that all twists lack $\mathbf{Q}_p$-points.

Theorem 2.15. *If $D \in S_p$ then for all $[\xi] \in H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathrm{Aut}(X_0^D(p)_{\mathbf{Q}}))$, and any twist $X_0^D(p)_\xi$ corresponding to $[\xi]$, $X_0^D(p)_\xi(\mathbf{Q}_p) = \emptyset$.*

Proof. Let $\{1, u, p, up\}$ denote representatives for the square classes of $\mathbf{Q}_p^\times$, $u = d_1$, $p = d_2$, and $\tau_1, \tau_2 \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $\tau_i(\sqrt{d_j}) = (-1)^{\delta_{ij}}\sqrt{d_j}$ with δ denoting the Kronecker delta function. Let $L = \mathbf{Q}_p(\sqrt{u}, \sqrt{p})$ and $\phi : \mathrm{Gal}(L/\mathbf{Q}_p) \to W$ be the homomorphism induced by ξ. If $\ker\phi \neq 0$, then $X_0^D(p)_\xi$ is a (possibly trivial) quadratic twist when we base change to $\mathbf{Q}_p$ and therefore lacks $\mathbf{Q}_p$-points. If $\ker\phi = 0$ then let $m_1, m_2 \mid Dp$ such that $\phi(\tau_i) = w_{m_i}$.

Suppose now to the contrary that there is a point $P \in X_0^D(p)(L)$ such that $\tau_i w_{m_i} P = P$. Then the reduction $\overline{P} \in X_0^D(p)(\mathbb{F}_{p^2})$ satisfies $\mathrm{Frob}_p\, w_{m_1}\overline{P} = \overline{P}$. It follows that $\overline{P}$ is supersingular by Lemma 2.9 and hence $\mathrm{Frob}_p\,\overline{P} = w_p\overline{P}$ [Sta14, Lemma 2.22]. Thus $\overline{P}$ is a fixed point of $w_p w_{m_1} = w_m$ where $m = pm_1/(p, m_1)^2$. It is also a fixed point of w_{m_2} since τ_2 acts as the identity on the $\overline{\mathbb{F}}_p$-points and thus of $w_n = w_m w_{m_2}$.

Now the Eichler embedding theorem [Cla03, Corollary 42] tells us that if $D \in S_p$ then m, m_2 and n all must be one of three possibilities (which we list only for m). They must also be distinct since $\ker\phi = 0$. Either

(1) $m = D$ or
(2) $m = Dp$ or

(3) $p \mid m$, $\omega(m)$ is even, and $\left(\frac{(m/p)}{p}\right) = 1$ (and in fact for all $q \mid (Dp/m)$, $\left(\frac{p}{q}\right) = -1$).

If $m = D$ and $m_2 = Dp$ then $n = p$, which does not fit into any of these three. If $m = D$ and m_2 fits (3) then $\left(\frac{(n/p)}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{(m_2/p)}{p}\right) = (-1)(1) = -1$ and n does not fit any of the possibilities. If $m = Dp$ and m_2 fits (3) then $\omega(n) \equiv \omega(m_2 Dp) \equiv 1 \bmod 2$ and again n fits none of these possibilities. Finally if both m and m_2 fit (3) then $p \nmid n$ so n would have to fit (1) but $n \neq D$ since that would mean $\left(\frac{D}{p}\right) = \left(\frac{(m/p)}{p}\right)\left(\frac{(m_2/p)}{p}\right) = 1$ while $\left(\frac{D}{p}\right) = -1$. Since the roles of m and m_2 are symmetric and $m \neq m_2$, we see that there is no such point P. □

Lemma 2.16. *For any $X \in \mathbf{Z}_{>0}$ and prime $p \equiv 1 \bmod 4$, $\#S_p(X) \gg X/\log(X)$.*

Proof. If we fix p, find some $q_1 > 4p$ such that $q_1 \equiv 1 \bmod 12$ $\left(\frac{q_1}{p}\right) = -1$ and for all $1 \leq s < \sqrt{4p}$, $\left(\frac{s^2 - 4p}{q_1}\right) = 1$. Fix q_1. Then the number of primes q_2 such that $q_1 q_2 \in S_p \cap \{1, \ldots, X\}$ is at least the number of primes $q_2 \equiv 1 \bmod 12pq_1$ which are greater then $4pq_1$ and less than X/q_1. This is asymptotic to $X/4(p-1)(q_1 - 1)q_1 \log(X)$ by the prime number theorem for arithmetic progressions. □

Proof of Theorem 2.1. For any $D \in S_p(X)$ for any $p \equiv 1 \bmod 4$, if T is a twist of $X_0^D(p)_{\mathbf{Q}}$ then $T(\mathbf{Q}_p) = \emptyset$. Since $\#S_p(X) \gg X/\log(X)$ the result follows. □

3. Torsors on Twists

Let $X^D(p)$ denote the moduli space of (A, ι, ν) where A is an abelian surface over a $\mathbf{Z}[1/p]$-scheme S, $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ where $\mathcal{O}$ is a maximal order in the quaternion algebra B of discriminant D and ν is a full-level p structure on (A, ι) for $p \nmid D$ [Dri76, Proposition 4.4]. That is, ν is an isomorphism between $A[p]$ and the constant group scheme $(\mathbf{Z}/p)^4$ with the structure of a free rank one left $\mathcal{O}/p$-module. There is an evident map $X^D(p) \to X^D$ induced by forgetting the level structure ν. Alternately, over an algebraically closed field of characteristic not p, there is a transitive Galois-equivariant action of $(\mathcal{O}/p)^\times \cong \mathrm{GL}_2(\mathbb{F}_p)$ on the set of ν above a fixed isomorphism class of a pair (A, ι). Here ± 1 acts trivially, the coarse quotient by $\mathrm{GL}_2(\mathbb{F}_p)/\pm 1$ is X^D, and the coarse quotient by the upper-triangular matrices is $X_0^D(p)$ [Cla03, p.38]. Note that $X^D(p)_{\mathbf{Q}}$ is not geometrically connected, and if we were to base change to the p-th cyclotomic field, it would split into a number of geometrically connected $\mathrm{PSL}_2(\mathbb{F}_p)$-covers. In any case, if D satisfies the conditions of Lemma 2.2 then $X_0^D(p)_{\mathbf{Q}}$ is an intermediate étale cover in the étale torsor $X^D(p)_{\mathbf{Q}} \to X^D_{\mathbf{Q}}$ under G where $G(\overline{\mathbf{Q}}) = \mathrm{GL}_2(\mathbb{F}_p)/\pm 1$. In fact there is a corresponding torsor over any quadratic twist by an Atkin-Lehner involution.

That is, if $m \mid D$, there is a unique two-sided ideal of norm m in $\mathcal{O}$ with principal generator β, unique up to unit multiplication on either side. If $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ and we let $\iota_m(b) = \iota(\beta^{-1} b \beta)$ [Sta12, Definition 2.2.2]. In fact, we can extend this to an action on $X^D(p)$ by setting $\nu_m(a) = \nu(\beta^{-1} a)$. This definition does not depend on the choice of generator β and we may choose a different one if it suits

us. Note that $p \nmid D$ so β^{-1} is a valid element of $(\mathcal{O}/p)^\times$. So let $[A, \iota, \nu]$ denote the isomorphism class of the triple, where an isomorphism from (A, ι, ν) to (A', ι', ν') is an isomorphism of abelian S-schemes $\phi : A \to A'$ such that $\phi\iota\phi^{-1} = \iota'$ and $\nu' = \phi\nu$. We let $K/\mathbf{Q}$ be a quadratic field and we let σ be the nontrivial Galois automorphism of $K/\mathbf{Q}$ where $K = \mathbf{Q}(\sqrt{d})$. By abuse of notation, we let σ denote the induced automorphism of abelian schemes $\sigma : A^\sigma \to A$. We similarly let $\iota^\sigma(b) = \sigma^{-1}\iota(b)\sigma$ and $\nu^\sigma(a) = \sigma^{-1}\nu(a)$.

Now consider $H_m \cong \mathbf{Z}/2$ acting on $X^D(p)_K$ with nontrivial element h sending $[A, \iota, \nu]$ to $[A^\sigma, \iota_m^\sigma, \nu_m^\sigma]$. We let $T^D(p, d, m) = X^D(p)_K/H_m$, which is a curve we can take as defined over $\mathbf{Q}$. Moreover, we again have a simply transitive action of a twist G' of G.

Lemma 3.1. *Suppose that D satisfies the conditions of Lemma 2.2. If $\gamma \in (\mathcal{O}/N)^\times$ fixes a pair $([A, \iota, \nu], [A^\sigma, \iota_m^\sigma, \nu_m^\sigma])$ where S is a K-scheme and A is an abelian S-scheme then $\gamma = \pm 1$.*

Proof. We already know this to be true for the set of isomorphism classes $[A, \iota, \nu]$: if $\nu_\gamma(b) = \nu(b\gamma)$ then $[A, \iota, \nu] = [A, \iota, \nu_\gamma]$ if and only if $\gamma = \pm 1$. Therefore, if we want to find a situation where $\gamma \neq \pm 1$ fixes a pair, we must find a triple (A, ι, ν) where $[A, \iota, \nu_\gamma] = [A^\sigma, \iota_m^\sigma, \nu_m^\sigma]$. We note immediately that this implies (A, ι) is w_m-fixed as $[A, \iota] = [A^\sigma, \iota_m^\sigma]$, so we can take $\beta^2 = -m$. Moreover, we have an isomorphism of S-schemes between A and A^σ, so we may without loss of generality assume that $A = A^\sigma$ and $\sigma : A \to A$ is an order two isomorphism. So let $\phi : A \to A$ be an isomorphism of S-schemes such that $\phi\iota\phi^{-1} = \iota_m^\sigma$ and $\phi\nu_\gamma = \nu_m^\sigma$. It follows that ϕ^2 is another isomorphism of S-schemes but now its conjugate by ι is $(\iota_m^\sigma)_m^\sigma = \iota$ and therefore ϕ^2 commutes with $\iota(\mathcal{O})$.

By definition, the center of a quaternion algebra over $\mathbf{Q}$ is $\mathbf{Q}$ itself so the centralizing automorphisms in $\iota(\mathcal{O})$ are ± 1. Since A lies over a characteristic zero scheme S, if $\iota(\mathcal{O})$ is not the full ring of endomorphisms, A must have CM by an imaginary quadratic field K. If this is the case, then there is an embedding from an order R of K into $\mathcal{O}$ [Sta12, Lemma 2.3.3]. In fact we know $K = \mathbf{Q}(\sqrt{-m})$ and the units are ± 1 since (A, ι) is w_m-fixed. But then we have $\phi^2 = \pm 1$. Again, since there are no fourth roots of unity in $\mathcal{O}$, there are no automorphisms of A commuting with $\iota(\mathcal{O})$ which square to -1.

If $\phi = \pm 1$ then $[A, \iota, \nu] = [A, \iota, \nu_\gamma]$ and $\gamma = \pm 1$. Clearly this is the case if $\phi \in \iota(\mathcal{O})$. If not, we derive a contradiction from the fact that $\phi^2\nu(B) = \nu(\beta^{-2}B\gamma^{-2})$ for all $B \in \mathcal{O}/p$. In particular, $\gamma^2 \equiv -1/m \bmod p$, so we can take $\beta \equiv 1/\gamma \bmod p$, and recall $\mathrm{End}^0(A)$ is $M_2(\mathbf{Q}(\sqrt{-m}))$ since (A, ι) is w_m-fixed. If $\phi \neq \pm 1$ then in here, it is conjugate to either $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, which are the rational canonical forms respectively when $\phi^2 = 1$ or $\phi^2 = -1$. We focus on the pertinent case where p is inert in $\mathbf{Q}(\sqrt{-m})$, so $\mathrm{End}(A[p]) \cong M_2(\mathbb{F}_{p^2})$. The same will hold when p is split. Embedding $\mathcal{O}/p$ into here via $\iota \bmod p$ gives a group isomorphic to $M_2(\mathbb{F}_p)$ and a full level p structure by acting additively on the identity of A. Since $(\mathcal{O}/p)^\times$ acts transitively on these, we may assume this is ν without loss of generality. Thus in saying $\phi\nu(B) = \pm\sigma\nu(\gamma B\gamma^{-1})$ for all $B \in \mathcal{O}/p$, we are saying that in $M_2(\mathbb{F}_{p^2})$, there is a matrix α such that $\alpha M\alpha^{-1}B \equiv \pm\sigma\gamma B\gamma^{-1} \bmod p$. Before reducing modulo p, we know that under ι, σ must send β to $u\beta$ where $u \in \mathcal{O}^\times$ has norm 1 and moreover σ sends u to u^{-1}. By the structure of the automorphisms of GL_2 [Die55, IV.1.III], σ must send $B \in \mathrm{GL}_2(\mathbb{F}_p)$ to $\pm NBN^{-1}$ where the ± 1

factor may depend on B and $N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ so B is sent to ± 1 times its classical adjoint. Now plug in $B = \gamma$ so we find $\alpha M \alpha^{-1} \gamma = \pm\sigma(\gamma) = \pm m\gamma^{-1}$ and thus M is conjugate to $\pm m^2$ times the identity. If we compare traces, we see this cannot be. Therefore $\phi = \pm 1$, $\gamma = \pm 1$ and the Lemma is proved. □

We note that if we fix an isomorphism between $G'(\overline{\mathbf{Q}})$ and $\mathrm{GL}_2(\mathbb{F}_p)/\pm 1$ then the quotient of $T^D(p,d,m)$ by the upper-triangular matrices in G' is $C^D(p,d,m)$ and the quotient by G' is $C^D(1,d,m)$. We have therefore transferred this "level structure torsor" on X^D over to its twist.

4. Descent Obstructions

Let us briefly review some facts about the descent obstruction.

Lemma 4.1. *Let V be a smooth, proper variety over $\mathbf{Q}$. Then we have a bijection of sets between $\prod_{p\leq\infty} V(\mathbf{Q}_p)$ and $V(\mathbf{A})$ where $\mathbf{A}$ denotes the adeles of $\mathbf{Q}$. Note that by the diagonal embedding we have $V(\mathbf{Q}) \subset V(\mathbf{A})$.*

Proof. [Sko01, pp.98-99] □

Definition 4.2. We say that a smooth, proper variety $V_{/\mathbf{Q}}$ is a *counterexample to the Hasse principle* or *Hasse principle violation* if $V(\mathbf{Q}) = \emptyset$ but $V(\mathbf{A}) \neq \emptyset$.

Let us return to our level-structure torsor. Recall now that the Galois twists of the torsor $X^D(p)_{\mathbf{Q}} \to X^D_{\mathbf{Q}}$ are given by the cohomology set $H^1(\mathrm{Gal}_{\mathbf{Q}}, G(\overline{\mathbf{Q}}))$. In particular, for all $[\zeta]$ in $H^1(\mathrm{Gal}_{\mathbf{Q}}, G(\overline{\mathbf{Q}}))$, there is an inner twist G_ζ and a twist $X^D(p)_\zeta$ such that $(X^D(p)_\zeta)_{\mathbf{Q}} \to X^D_{\mathbf{Q}}$ is an étale torsor under G_ζ. The same is true for $T^D(p,d,m) \to C^D(1,d,m)$. For all ζ we get a twisted torsor $T^D(p,d,m)_\zeta \to C^D(1,d,m)$ under G'_ζ. Moreover, this torsor factors through a twist of $C^D(p,d,m)$ because we can simply take the quotient by the upper-triangular subgroup of G'_ζ.

Definition 4.3. [Sko01, Definition 5.3.1] Let G be a linear algebraic group (e.g., a finite group scheme) over $\mathbf{Q}$ and let $f : Y \to X$ be a torsor under G. It follows that we have an intermediate set $X(\mathbf{Q}) \subset \kappa(f) \subset X(\mathbf{A})$ defined as

$$\kappa(f) = \bigcup_{[\zeta]\in H^1(\mathrm{Gal}_{\mathbf{Q}}, G(\overline{\mathbf{Q}}))} f_\zeta(Y_\zeta(\mathbf{A})).$$

We call this set the *descent obstruction* associated to the torsor f.

Theorem 4.4. *If X is an Atkin-Lehner twist of X^D with $D \in S = \bigcup_p S_p$ (Definition 2.14) then $X(\mathbf{Q}) = \emptyset$. Moreover if X is such that $X(\mathbf{A}) \neq \emptyset$ then X is a counterexample to the Hasse principle.*

Proof. If $X = C^D(1,d,m)_{\mathbf{Q}}$ is such a twist then for all $[\zeta] \in H^1(\mathrm{Gal}_{\mathbf{Q}}, G(\overline{\mathbf{Q}}))$ the twist Z_ζ of $Z = C^D(p,d,m)_{\mathbf{Q}}$ is a twist of $X_0^D(p)_{\mathbf{Q}}$ for some p. By Theorem 2.1, all such twists have $Z_\zeta(\mathbf{Q}_p) = \emptyset$. If we take $Y = T^D(p,d,m)$ then $Y_\zeta(\mathbf{Q}_p)$ surjects onto $Z_\zeta(\mathbf{Q}_p)$, so $Y_\zeta(\mathbf{Q}_p) = \emptyset$. It follows that $Y_\zeta(\mathbf{A}) = \emptyset$ and thus $\kappa(f) = \emptyset$. Since $X(\mathbf{Q}) \subset \kappa(f)$ [Sko01, §5.3], the result follows. □

Lemma 4.5. *Let Y be a variety over a field K and w a K-rational involution such that the quotient Z is also a variety over K. Then if all twists of Y by w have no K-rational points, Z has no K-rational points.*

Proof. Let $F \subset Y$ be the subscheme of fixed points of w, which we identify with its image B in Z. Let V be the complement of F and U the complement of B so $V \to U$ is a torsor under $\mathbf{Z}/2$. It follows that for all $[\zeta] \in H^1(\mathrm{Gal}_K, \langle w \rangle)$, $U(K) = \coprod_{[\zeta]} V_\zeta(K)$ [Sko01, p. 22]. Therefore

$$Z(K) = B(K) \cup U(K) = F(K) \cup \coprod_{[\zeta]} V_\zeta(K) \subset \bigcup_{[\zeta]} (V_\zeta(K) \cup F(K)) = \bigcup_{[\zeta]} Y_\zeta(K).$$

□

Proof of Theorem 1.1. Note that if $D \in S_p$ for some $p \equiv 1 \bmod 4$ then D is *untangled* (Definition 2.12). By Eichler's embedding theorem [Cla03, Corollary 42], this means there are no twisting elements in the quaternion algebra $B_{/\mathbf{Q}}$ of discriminant D and thus B is non-twisting in the sense of Rotger [Rot04, p.12]. Hence if the algebraic curve $X^D/\langle w_D \rangle$ has no $\mathbf{Q}$-rational points then there are no abelian surfaces $A_{/\mathbf{Q}}$ such that $B_D \hookrightarrow \mathrm{End}^0(A_{\overline{\mathbf{Q}}})$ [Cla03, Corollary 84]. By Theorem 4.4, for all twists X of X^D with $D \in S_p$ we have $X(\mathbf{Q}) = \emptyset$. By Lemma 4.5, $X^D/\langle w_D \rangle(\mathbf{Q}) = \emptyset$. By Lemma 2.16, $S_p(X)$ is large enough to complete the proof for all $p \equiv 1 \bmod 4$. □

5. Bounds for Adelic points

We now work somewhat more generally and show both upper and lower bounds for twists of Shimura curves with adelic points. We observe that there is a sense in which almost all quadratic twists of a Shimura curve fail to have adelic points. Throughout, let D be the discriminant of a quaternion algebra in $M_2(\mathbf{R})$. For all such D, $X^D(\mathbf{R}) = \emptyset$ [Shi75], and so in particular, all twists by real quadratic fields fail to have adelic points. Second, it is conjectured to be the case that with only finitely many exceptions [KR08] there are only Atkin-Lehner automorphisms and by adapting the proof of Theorem 2.4 we can show that if D is untangled then there are no adelic points on any twists except the twists by w_D. Still, even when we restrict to twists by w_D and $\mathbf{Q}(\sqrt{d})$ with $d < 0$, we find that *almost all* twists lack adelic points. In the following, we define $C^D(1, d, D)$ as the twist of X^D defined by the cocycle $\xi \in H^1(\mathrm{Gal}_{\mathbf{Q}}, \mathrm{Aut}(X^D))$ which is induced by the isomorphism $\mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q}) \cong \langle w_D \rangle$.

Definition 5.1. If Σ is a set of negative integers, let $\Sigma(X) = \Sigma \cap \{-X, \ldots, -1\}$. If $\#\Sigma(X) = o(X)$, then we say that almost all negative integers are not in Σ. Let Σ_D be the collection of $d < 0$ such that $C^D(1, d, D)(\mathbf{A}) \neq \emptyset$

Lemma 5.2. *There is a real number $0 < \tau < 1$ such that $\#\Sigma_D(X) \ll X/\log^\tau(X)$ and in particular, almost all twists of X^D do not have adelic points.*

Proof. This is a straightforward application of known results on points at ramified primes [Sta14, Theorem 4.1] and an old result exposed by Serre [Ser76, Théorème 2.8] on Chebotarev sets. Let $H_\Delta(X)$ be the Hilbert class polynomial for $\mathbf{Z}[(\Delta + \sqrt{\Delta})/2]$.

Consider the set C of primes containing the primes dividing $2D$ and those satisfying parts 1-3 of the result on ramified primes [Sta14, Theorem 4.1] (if D is even, substitute part 5 for part 3). We note first that if $H_{-4D}(T)$ has a root $\bmod p$ then so does $H_{-D}(T)$ under the hypothesis $D \equiv 3 \bmod 4$ because there is a containment of the fields generated by their roots over $\mathbf{Q}$. Moreover, at least 2 primes divide

D so there is always a quadratic subextension of this field [Cox89, Theorem 6.1]. If we let $h(\Delta) = \deg H_\Delta(T)$ then $1/2h(-4D) \leq 1/2h(-D)$ so at most the density of primes satisfying parts 1 and 2 is $1/h(-D) \leq 1/2$ if $D \equiv 3 \bmod 4$ and at most $1/2h(-4D) \leq 1/4$ if $D \equiv 1, 2 \bmod 4$. Let $\omega(n)$ be the number of distinct prime divisors of n. The primes satisfying part 3 or 5 are given by congruence conditions and have density at most $(1/2)^{\omega(D)} \leq 1/4$. Therefore the density of C in the set of all primes is a real number $0 < \tau' < 1$ and we may apply Serre's theorem to get our asymptotic upper bound on $\Sigma_D(X)$ with $\tau = 1 - \tau'$. □

In the above, the value of τ depends on $D \bmod 4$. If $D \equiv 1 \bmod 4$, for instance if $D \in S = \bigcup_p S_p$ (Definition 2.14), then we can take

$$\tau' = \frac{1}{2h(-4D)} + (1/2)^{\omega(D)} < (1/2)^{\omega(D)-1}.$$

Moreover, by Theorem 4.4, if $D \in S$ then Σ_D is the set of d for which $C^D(1, d, D)$ is a counterexample to the Hasse Principle.

Having given asymptotic upper bounds, let us show how to find twists of X^D which have adelic points. Let I be the product of the primes less than $4g(X^D)^2$ which do not divide $2D$. Let u_i be the set of elements between 1 and I such that $\left(\frac{u_i}{\ell}\right) = -1$ for all $\ell \mid I$. Similarly, let $\{v_j\}$ be the set of elements between 1 and $8D$ (or $4D$ if D is even, but for now let's assume D is odd) such that $v_j \equiv 3 \bmod 8$ and for all $q \mid D$ odd, $\left(\frac{v_j}{q}\right) = -1$. Note that the number of such v_j is $(1/4)(1/2)^{\omega(D)}\phi(8D)$. Let also μ be the Möebius function and let b_n be the multiplicative function such that if p is prime,

$$b_{p^m} = \begin{cases} 1 & p \equiv v_j \bmod 8D \text{ for some } j \\ 0 & else. \end{cases}$$

We let

$$a_n = b_n \left(\frac{1}{\phi(I)} \sum_\chi \sum_i \overline{\chi(-u_i)}\chi(n) \right) \left(\frac{\mu^2(n) - \mu(n)}{2} \right),$$

where χ runs over the $\bmod I$ Dirichlet characters.

Here $a_n = 1$ if $-n \equiv u_i \bmod I$ for some i, n (and thus $-n$) is square-free with an odd number of prime factors, and each prime dividing n is congruent to some v_j. If not, $a_n = 0$. Let η_D be the collection of discriminants d such that $a_{-d} = 1$, so that $\#\eta_D(X) = \sum_{n \leq X} a_n$.

Lemma 5.3. *If $g(X^D) > 3$ and $d \in \eta_D$ then $C^D(1, d, D)(\mathbf{A}) \neq \emptyset$, i.e., $\eta_D \subset \Sigma_D$.*

Proof. First we show that if $D \notin E = \{6, 10, 14, 15, 21, 22, 33, 34, 38, 46, 58, 82, 94\}$ and $g = g(X^D)$ then for all $p \mid D$, $p < 4g^2$. Note that if D is in the exceptional set E then $g(X^D) \leq 3$, and if D is not exceptional while $g(X^D) \leq 2$ then $D = 26$. In particular each X^D with $D \in E$ is a double cover of $\mathbb{P}^1$ over $\overline{\mathbf{Q}}$, and unless $D = 82$ each X^D is hyperelliptic over $\mathbf{Q}$, so we can produce twists with rational points by other means. Recall that for $D > 1$ [Cla03, Proposition 46],

$$g = 1 + \frac{\varphi(D)}{12} - \frac{e_2}{4} - \frac{e_3}{3} \geq \frac{12 + \phi(D) - 7(2^{\omega(D)})}{12}.$$

This implies that

$$4g^2 \geq \frac{1}{36}(12 + \varphi(D) - 7(2^{\omega(D)}))^2.$$

Therefore to say that $p < 4g^2$ it is enough to require that

$$6\sqrt{p} < 12 + \varphi(D) - 7(2^{\omega(D)}).$$

Let $D = pq$ with $p < q$. It follows that $(q-1) \leq \varphi(D)$ with equality precisely when $p = 2$. Therefore $12 + \varphi(D) - 7(4) \geq (q-1) - 16 = q - 17$ and $q - 17 > 6\sqrt{q} \geq 6\sqrt{p}$ if $q > 66$. We may now easily compute the exceptional $D = pq$.

For the general case, note that $\varphi(D) - 7(2^{\omega(D)}) \geq 6\sqrt{D}$ if and only if

$$\left(\prod_{p|D} \frac{p-1}{2}\right) - 7 \geq 6\sqrt{\prod_{p|D} p/4}.$$

If y is a real number then $(y-1)/2 \geq y/4$ if and only if $y \geq 2$, for instance if y is a prime number. So if $\alpha(D) - 7 \geq 6\sqrt{\alpha(D)}$ for $\alpha(D) = \prod_{p|D} \frac{p-1}{2}$ then $\varphi(D) - 7(2^{\omega(D)}) \geq 6\sqrt{D} \geq 6\sqrt{p}$ for all $p \mid D$. We are therefore done unless $\alpha(D) \leq 49$. If $\omega(D) = 4$ then we find our largest prime divisor q must be at most 97 and we compute that there are no exceptional D in this range. If $\omega(D) \geq 6$, we find $q \leq \frac{113}{15} = 7.5\underline{3}$, a contradiction.

In any case [Sta14, Corollary 3.17, Corollary 5.2], if $d < 0$ is a square-free integer such that $\left(\frac{d}{\ell}\right) = -1$ for all primes $\ell < 4g^2$, then $C^D(1, d, D)(\mathbf{Q}_\ell) \neq \emptyset$ for all primes $\ell \nmid d$ including ∞. If $r \mid d$ is prime, $r \equiv 3 \bmod 8$, and $\left(\frac{-r}{q}\right) = -1$ for all $q \mid D$ then $C^D(1, d, D)(\mathbf{Q}_r) \neq \emptyset$ if $\left(\frac{-D}{r}\right) = -1$ [Sta14, Theorem 4.1]. Since there are an even number of divisors of D and $\left(\frac{-r}{q}\right) = \left(\frac{q}{r}\right)$, we have $\left(\frac{-D}{r}\right) = -1$. Therefore if $d \in \eta_D$, all primes dividing d are of this form. □

Lemma 5.4. *There is a positive constant c_D depending only on D such that if $\alpha = 1 - (1/2)^{\omega(D)+2}$ when D is odd and $1 - (1/2)^{\omega(D)+1}$ when D is even, the number of discriminants $-1 \leq d \leq -X$ with the properties we want is*

$$\#\eta_D(X) = c_D X/\log^\alpha(X) + O(X/\log^{1+\alpha}(X)).$$

Proof. Consider the function $f(s) = \sum_n a_n n^{-s}$, holomorphic on $\Re(s) > 1$. Despite the way it is written, $f(s)$ is not a Dirichlet series as the a_n are not necessarily multiplicative. We however reduce to this case as we write the Dirichlet series $f_{k,\chi}(s) = \sum_{n \geq 0} b_n \mu^k(n)\chi(n)n^{-s}$, again converging in the half-plane $\Re(s) > 1$. We therefore have

$$f(s) = \frac{1}{2\phi(I)} \sum_\chi \left(\left(\sum_i \overline{\chi(-u_i)} \right) (f_{2,\chi}(s) - f_{1,\chi}(s)) \right).$$

We begin by showing that with the exception of $(k, \chi) = (2, \mathbb{1})$, these are in fact holomorphic for $\Re(s) \geq 1$.

Consider

$$\begin{aligned}\log(f_{k,\chi}(s)) &= \sum_p \log(\sum_{m\geq 0} b_{p^m}\mu^k(p^m)\chi(p^m)p^{-ms}) \\ &= \sum_p \log(1+b_p(-1)^k\chi(p)p^{-s}) \\ &= (-1)^k\sum_p \frac{b_p\chi(p)}{p^s} + \beta_{k,\chi}(s)\end{aligned}$$

where $\beta_{k,\chi}(s)$ is holomorphic on $\Re(s) > 1/2$.
Now use the fact that (again assuming D is odd)

$$b_p = 1/\phi(8D)\sum_{\psi \bmod 8D}\sum_j \overline{\psi(v_j)}\psi(p).$$

Therefore

$$\log(f_{k,\chi}(s)) = (-1)^k\frac{1}{\phi(8D)}\sum_\psi\sum_j \overline{\psi(v_j)}\log(L(s,\chi\psi)) + \rho_{k,\chi}(s),$$

where $\rho_{k,\chi}$ is holomorphic for $\Re(s) > 1/2$.

It follows that zero-free regions for L-functions of Dirichlet characters give zero-free regions for the $f_{j,\chi}$ and thus holomorphic regions for f. In particular, if ϵ is a Dirichlet character and $\delta_\epsilon = 1$ for $\epsilon = \mathbb{1}$ and zero otherwise then there are positive numbers A_ϵ, b_ϵ such that $\log(L(s,\epsilon)) - \delta_\epsilon\log(1/(s-1))$ is holomorphic on $\Re(s) \geq 1 - b_\epsilon/\log^{A_\epsilon}(2+|\Im(s)|)$ [Ser76, Proposition 1.7].

Now we note that since $(I, 8D) = 1$, $\chi\psi = \mathbb{1}$ if and only if $\chi = \mathbb{1}$ and $\psi = \mathbb{1}$. Therefore by exponentiating, we find a holomorphic, nonzero function $g_{k,\chi}$ on the same region in $\mathbf{C}$ such that $f_{k,\chi}(s) = \left(\frac{1}{(s-1)}\right)^{\frac{\delta_\chi(-1)^k}{2^{\omega(D)+2}}} g_{k,\chi}(s)$.

Therefore, there is a function g holomorphic on the intersection of the A_ϵ, b_ϵ regions such that $f(s) = \left(\frac{1}{(s-1)}\right)^{\frac{1}{2^{\omega(D)+2}}} g(s)$. Finally, we may apply the method of Serre and Watson [Ser76, Théorème 2.8] to get our asymptotic for $\sum_{n\leq X} a_n$. □

Note that by combining Lemma 5.2 with Lemma 5.4, we can say that for all $D \in S$,

$$X/\log^{1-(1/2)^{\omega(D)-1}}(X) \gg \#\Sigma_D(X) \geq \#\eta_D(X) \gg X/\log^{1-(1/2)^{\omega(D)+2}}(X).$$

We see therefore that the set η_D is nearly optimal. More to the point, we can complete our final proof.

Proof of Theorem 1.2. For all $D \in S$ and $d \in \eta_D(X)$, take $T = C^D(1,d,D)$. By Lemma 5.4, $\eta_D(X)$ has the correct size and $T(\mathbf{A}) \neq \emptyset$. By Theorem 4.4, $T(\mathbf{Q}) = \emptyset$ because the descent obstruction set is empty. □

References

[Bak68] A. Baker, *Linear forms in the logarithms of algebraic numbers. IV*, Mathematika **15** (1968), 204–216.

[BFGR06] Nils Bruin, E. Victor Flynn, Josep González, and Victor Rotger, *On finiteness conjectures for endomorphism algebras of abelian surfaces*, Math. Proc. Cambridge Philos. Soc. **141** (2006), no. 3, 383–408.

[Bha] M. Bhargava, *Most hyperelliptic curves over q have no rational points*, Preprint.

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990.

[Cla03] Pete L. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*, ProQuest LLC, Ann Arbor, MI, 2003, Thesis (Ph.D.)–Harvard University.

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[Die55] Jean Dieudonné, *La géométrie des groupes classiques*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), Heft 5, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[Dri76] V. G. Drinfel'd, *Coverings of p-adic symmetric domains*, Funkcional. Anal. i Priložen. **10** (1976), no. 2, 29–40.

[dVP13] Carlos de Vera-Piquero, *The Shimura covering of a Shimura curve: automorphisms and étale subcoverings*, J. Number Theory **133** (2013), no. 10, 3500–3516.

[Eic56] Martin Eichler, *Modular correspondences and their representations*, J. Indian Math. Soc. (N.S.) **20** (1956), 163–206.

[Gau86] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Hee52] Kurt Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

[JL85] Bruce W. Jordan and Ron A. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. **270** (1985), no. 2, 235–248.

[KR08] Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 363–374.

[Lor14] Dino Lorenzini, *Wild models of curves*, Algebra Number Theory **8** (2014), no. 2, 331–367.

[Mol12] Santiago Molina, *Ribet bimodules and the specialization of Heegner points*, Israel J. Math. **189** (2012), 1–38.

[Mor12] Masanori Morishita, *Knots and primes*, Universitext, Springer, London, 2012.

[Rot02] Victor Rotger, *On the group of automorphisms of Shimura curves and applications*, Compositio Math. **132** (2002), no. 2, 229–241.

[Rot04] ———, *Shimura curves embedded in Igusa's threefold*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 263–276.

[RSY05] Victor Rotger, Alexei Skorobogatov, and Andrei Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$*, Mosc. Math. J. **5** (2005), no. 2, 463–476, 495.

[Ser76] Jean-Pierre Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. (2) **22** (1976), no. 3-4, 227–260.

[Shi75] Goro Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.

[Sko05] ———, *Shimura coverings of Shimura curves and the Manin obstruction*, Math. Res. Lett. **12** (2005), no. 5-6, 779–788.

[Sta67] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1–27.

[Sta12] James Stankewicz, *Twists of Shimura curves*, 2012, Thesis (Ph.D.)–University of Georgia.

[Sta14] ———, *Twists of Shimura curves*, Canad. Jour. Math. **66** (2014), no. 4, 924–960.

[Sta15] The Stacks Project Authors, *stacks project*, `http://stacks.math.columbia.edu`, 2015.

[Wat35] G. N. Watson, *Über Ramanujansche Kongruenzeigenschaften der Zerfällungsanzahlen. (I)*, Math. Z. **39** (1935), no. 1, 712–731.

University of Bristol and Heilbronn Institute for Mathematical Research